I385557

公告本

100 年 12 月 23 日替換頁

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：95148822

※ 申請日期：95.12.25　　※IPC 分類：G06F21/24 (2006.01)
G06F17/50 (2006.01)

一、發明名稱：（中文/英文）

應用於控制晶片之程式碼開發程式中之資料保護方法與工具程式

DATA SECURING METHOD AND PROGRAM FOR USE IN PROGRAM CODE DEVELOPMENT TOOL FOR CONTROL CHIP

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

威盛電子股份有限公司/VIA TECHNOLOGIES, INC.

代表人：（中文/英文）王雪紅/WANG, CHER

住居所或營業所地址：（中文/英文）

新北市新店區中正路 533 號 8 樓

8F, 533, Zhongzheng Rd., Xindian Dist., New Taipei City 231, Taiwan, R.O.C.

國　籍：（中文/英文）中華民國/TW

三、發明人：（共 1 人）

姓　名：（中文/英文）

1.吳宗憲/WU, TSUNG HSIEN

國　籍：（中文/英文）

1.中華民國/TW

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

五、中文發明摘要：

本案係為一種資料保護方法，應用於一工具程式中，該方法包含下列步驟：接收一第一輸入資料進行一第一處理步驟而產生一第一輸出資料；將該第一輸出資料透過一流程控制器之轉傳而進行一加密動作，進而產生一第一輸出加密資料；將該第一輸出加密資料透過該流程控制器之轉傳來進行一解密動作，進而還原成一第一輸出解密資料；以及將該第一輸出解密資料進行一第二處理步驟而產生一第二輸出資料。

六、英文發明摘要：

A data securing method for use in a program tool includes steps of: receiving a first input data for a first processing procedure to obtain a first output data; performing an encryption operation of the first output data while being transferred via a flow controller to obtain a first encrypted output data; performing a decryption operation of the first encrypted output data while being transferred via the flow controller to obtain a first decrypted output data; and processing the first decrypted output data with a second processing procedure to generate a second output data.

七、指定代表圖：

(一)本案指定代表圖為：第四圖。

(二)本代表圖之元件符號簡單說明：

第一處理步驟 41

第一輸出資料 411

編碼步驟 402

第一輸出加密資料 491

第一輸出解密資料 471

第二輸出資料 421

第二輸出加密資料 492

第四輸入資料 4302

第五輸入資料 430

第三輸出資料 431

第三加密/解密動作 483

第三輸出解密資料 473

第一輸入資料 410

流程控制步驟 401

第一加密/解密動作 481

第二輸入資料 420

第二處理步驟 42

第二加密/解密動作 482

第三輸入資料 4301

第二輸出解密資料 472

第三處理步驟 43

記憶體裝置 45

第三輸出加密資料 493

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

九、發明說明：

【發明所屬之技術領域】

本案係為一種資料保護方法，尤指應用於工具程式中一資料保護方法。

【先前技術】

大部份的電子產品都是由許多電路模組所組成，而隨著分工程度的增加，同一電子產品內的電路模組極可能皆分別由不同公司所設計、製造。以第一圖中所示之行動電話手機為例，其主要由射頻/中頻模組 11、基頻/控制模組 12、記憶體模組 13、輸入鍵盤模組 14、音頻模組 15 以及顯示器模組 16 等元件構成，而行動電話手機製造商便向各個元件的製造商購買零件來進行整合與組裝。而其中基頻/控制模組 12 中具有一核心元件-系統單晶片 120，行動電話手機製造商向積體電路設計公司購買其設計之系統單晶片 120 後，便可以其為核心來設計其行動電話手機，而行動電話手機製造商可透過中階或高階程式碼的撰寫，來對該系統單晶片 120 進行功能設計與調整。

而為能方便系統製造商對該系統單晶片 120 進行程式改寫，積體電路設計公司便會提供一個工具程式給系統製造商來運用。請參見第二圖，其係一習用工具程式執行時之流程示意圖，其中第一處理步驟 21 接收第一輸入資料

210 進行處理後產生的第一輸出資料 211 會被送入第二處理步驟 22 進行處理，第二處理步驟 22 接收第一輸出資料進行處理後產生的第二輸出資料則再被送入第三處理步驟 23 進行處理，而第三處理步驟 23 可對第二輸出資料 221 與第三輸入資料 230 進行處理而產生第三輸出資料 231，至於第四處理步驟 24 可接收第三輸出資料 231 進行處理後，將其最後產生的可用以控制該系統單晶片 120 之程式碼送入記憶體 25 中儲存。而相對應各處理步驟之節點 201、202、203 及 204 係代表該工具程式之進入點，意即系統製造商可以任意由上述節點來進入該程式之處理流程來進行程式碼之解讀或編輯。

但如此一來，透過節點 201、202、203 及 204，工具程式之使用者可輕易知道上述處理步驟所產生之中間產物的內容，例如上述第一輸出資料 211、第二輸出資料 221 及第三輸出資料 231 之內容，導致上述系統單晶片 120（例如具有數位信號處理（DSP）功能的嵌入式精簡指令集（RISC）微處理器）之技術內容（例如指令集之詳細內容）被知悉過多，而如何改善此一習用手段缺失，係為發展本案之主要目的。

【發明內容】

本案係為一種資料保護方法，應用於一工具程式中，該方法包含下列步驟：接收一第一輸入資料進行一第一處

理步驟而產生一第一輸出資料；將該第一輸出資料透過一流程控制器之轉傳而進行一加密動作，進而產生一第一輸出加密資料；將該第一輸出加密資料透過該流程控制器之轉傳來進行一解密動作，進而還原成一第一輸出解密資料；以及將該第一輸出解密資料進行一第二處理步驟而產生一第二輸出資料。

本案之另一方面係為一種資料保護工具程式，用以處理經過加密之一輸入資料，包括：複數處理單元，該複數處理單元分別進行對應之複數處理步驟；其中，該輸入資料進行一解密步驟後執行任一處理步驟以產生一輸出資料；及該輸出資料進行再次加密。而其中該輸出資料於再次加密後自與執行之該處理步驟對應之該處理單元輸出。至於該輸出資料可為另一處理單元之該輸入資料。而該輸入資料進行一解密步驟後執行任一處理步驟以產生另一輸出資料；及該輸出資料進行再次加密。

另外，自該資料保護工具程式輸出之該輸出資料為加密的狀態。

【實施方式】

由於習知對於處理加密資料的觀念，僅是將最後的輸出資料進行加密來達到資料保密的效果。而若是工具程式中有數個處理單元來進行對應處理步驟時，對於每一處理步驟間所產生之中間產物則並未能提供加密動作以及整體

之流程控制，因此無法達到完全保護與保密之目的，而本案之主要特徵便在於，當工具程式中有數個處理單元來進行對應處理步驟時，從每一處理單元輸出之處理後的輸入資料都會進行資料保護編碼後才能暫存以及提供存取，並在輸至下一處理單元時再解密以進行對應處理步驟。這樣的作法便可降低處理過程中資料被改動或竊取的風險。

因此本案所發展出來之資料保護工具程式，其係用以處理經過加密之一輸入資料，本案之工具程式包括：複數處理單元，該複數處理單元分別進行對應之複數處理步驟；其中，該輸入資料進行一解密步驟後執行任一處理步驟以產生一輸出資料；及該輸出資料進行再次加密。而其中該輸出資料於再次加密後自與執行之該處理步驟對應之該處理單元輸出，至於該輸出資料可為另一處理單元之該輸入資料，而該輸入資料進行一解密步驟後執行任一處理步驟以產生另一輸出資料；而該輸出資料可進行再次加密。另外，自該資料保護工具程式輸出之該輸出資料為加密的狀態。而為能更了解此一概念，係以下列圖文舉例說明。

請參見第三圖，其係為改善習用控制晶片之程式碼開發程式（以下簡稱工具程式）缺失所發展出之本案工具程式之功能方塊示意圖，其中表示出了 3 個處理元件（當然可以更多）：第一處理元件 301、第二處理元件 302 以及第三處理元件 303，其係分別代表工具程式中用以進行第一處理步驟、第二處理步驟以及第三處理步驟之模組。而使

用者將第一輸入資料送入第一處理元件 301 進行第一處理步驟所產生之第一輸出資料，會馬上被本案所增設之流程控制器 31 轉傳至第一加密/解密模組 321 重新進行加密編碼而形成一第一輸出加密資料後才可被暫存成一檔案而可提供存取。然後，當使用者想將第一輸出加密資料及/或與第一輸出加密資料相同編碼規則之第二輸入資料送進第二處理元件 302 進行第二處理步驟來產生第二輸出資料時，流程控制器 31 會先將第一輸出加密資料及/或該第二輸入資料轉傳至第一加密/解密模組 321 進行解密解碼而還原成該第一輸出資料及/或解密後之該第二輸入資料後再被送入第二處理元件 302 進行第二處理步驟而產生一第二輸出資料。同樣地，第二輸出資料會馬上被本案所增設之流程控制器 31 轉傳至第二加密/解密模組 322 重新進行加密編碼而形成一第二輸出加密資料後才可被暫存成一檔案而可提供存取。再來，當使用者想將第二輸出加密資料及/或與第二輸出加密資料相同編碼規則之第三輸入資料送進第三處理元件 303 進行第三處理步驟來產生第三輸出資料時，流程控制器 31 會先將第二輸出加密資料及/或該第三輸入資料轉傳至第二加密/解密模組 322 進行解密解碼而還原成該第二輸出資料及/或解密後之該第三輸入資料後再被送入第三處理元件 303 進行第三處理步驟而最後產生一第三輸出資料送出，同樣地，第三輸出資料也可被流程控制器 31 轉傳至第三加密/解密模組 323 重新進行加密編碼而形成一第三輸出加密資料後被儲存，而要被存取使用時，再

透過第三加密/解密模組 323 進行解密解碼來進行還原。如此一來，中間產物與最後產物之資料皆被完整加密而能確保不被盜取或改動。

再請參見第四圖，其係一本案構思之工具程式執行時之流程示意圖，其中第一處理步驟 41 接收第一輸入資料 410 進行處理後產生的第一輸出資料 411 會被流程控制步驟 401 及編碼步驟 402 來控制，轉而進行第一加密/解密動作 481 中之加密動作，進而產生第一輸出加密資料 491 來進行暫存，而使用者僅能對第一輸出加密資料 491 進行存取與檢視，而工具程式便可利用加密之機制來提供部份資料可供使用者進行檢視，但部份資料則被隱藏，於是可達到中間資料保護與保密之作用。

再者，第一輸出加密資料 491 及/或與第一輸出加密資料相同編碼規則之該第二輸入資料 420 皆可透過流程控制步驟 401 與編碼步驟 402 之轉傳來進行第一加密/解密動作 481 之解密動作而還原成該第一輸出解密資料 471 後，再傳至第二處理步驟 42 進行處理，用以產生第二輸出資料 421 後再送入流程控制步驟 401 及編碼步驟 402 而進行第二加密/解密動作 482 中的加密動作，進而產生第二輸出加密資料 492 來進行暫存。

而暫存之第二輸出加密資料 492 及/或與第二輸出加密資料相同編碼規則之該第三輸入資料 4301 與第四輸入資料 4302 等中間產物，其皆可透過流程控制步驟 401 與編碼步驟 402 之轉傳來進行第二加密/解密動作 482 之解密動作

而還原成第二輸出解密資料 472 後，再與另外可能存在之第五輸入資料 430 一起送入第三處理步驟 43 進行處理，進而產生最終產物-第三輸出資料 431，而內容是程式碼之第三輸出資料 431 便可進行第三加密/解密動作 483 中的加密動作而形成一第三輸出加密資料 493 後再被送入一記憶體裝置 45（例如是快閃記憶體或其它非揮發性記憶體）進行儲存，最後形成可用以控制該控制晶片之韌體，而要使用時再從記憶體裝置 45 中讀取並進行第三加密/解密動作 483 中的解密動作來產生第三輸出解密資料 473。另外，雖然本例是以三個處理步驟來進行說明，但是擴充至四個或四個以上的處理步驟也是沒有問題的，因此不再贅述。

如此一來，使用者（例如系統製造商）便無法任意進入該工具程式之處理流程來進行全部程式碼之解讀或編輯，而是在工具程式提供者的控制下來進行程式碼之解讀或編輯，因此本案所發展出來之工具程式的使用者無法輕易知道上述處理步驟所產生之中間產物的全部內容，進而達成控制部份功能不能被使用者改動而部份功能可以被使用者而改動之目的。因此本案確實可改善習用手段缺失，進而達成發展本案之主要目的。而本發明可廣泛應用至各式具有控制晶片之電子產品之程式碼開發工具程式中，因此本案得由熟習此技藝之人士任施匠思而為諸般修飾，然皆不脫如附申請專利範圍所欲保護者。

【圖式簡單說明】

本案得藉由下列圖式及說明，俾得一更深入之了解：

第一圖，其係具有系統單晶片之行動電話手機功能方塊示意圖。

第二圖，其係習用工具程式執行時之流程示意圖。

第三圖，其係本案工具程式之功能方塊示意圖。

第四圖，其係一本案構思之工具程式執行時之流程示意圖。

【主要元件符號說明】

本案圖式中所包含之各元件列示如下：

射頻/中頻模組 11	基頻/控制模組 12
記憶體模組 13	輸入鍵盤模組 14
音頻模組 15	顯示器模組 16
系統單晶片 120	
第一處理步驟 21	第一輸入資料 210
第一輸出資料 211	第二處理步驟 22
第三處理步驟 23	第二輸出資料 221
第三輸入資料 230	第三輸出資料 231
第四處理步驟 24	節點 201、202、203 及 204
記憶體 25	
第一處理元件 301	第二處理元件 302
第三處理元件 303	第一加密/解密模組 321
第二加密/解密模組 322	第三加密/解密模組 323

流程控制器 31

第一處理步驟 41

第一輸出資料 411

編碼步驟 402

第一輸出加密資料 491

第一輸出解密資料 471

第二輸出資料 421

第二輸出加密資料 492

第四輸入資料 4302

第五輸入資料 430

第三輸出資料 431

第三加密/解密動作 483

第三輸出解密資料 473

第一輸入資料 410

流程控制步驟 401

第一加密/解密動作 481

第二輸入資料 420

第二處理步驟 42

第二加密/解密動作 482

第三輸入資料 4301

第二輸出解密資料 472

第三處理步驟 43

記憶體裝置 45

第三輸出加密資料 493

十、申請專利範圍：

1.一種資料保護方法，應用於提供一第一處理元件與一第二處理元件之一工具程式中，該方法包含下列步驟：

接收一第一輸入資料進行一第一處理步驟而於該第一處理元件產生一第一輸出資料；

將該第一輸出資料透過一流程控制器之轉傳而進行一加密動作，進而產生一第一輸出加密資料；

將該第一輸出加密資料透過該流程控制器之轉傳來進行一解密動作，進而還原成一第一輸出解密資料；以及

將該第一輸出解密資料進行一第二處理步驟而於該第二處理元件產生一第二輸出資料，其中該第一輸出加密資料係為該第一處理元件與該第二處理元件間之中間資料以供使用者存取，而該第一輸出解密資料不可被使用者存取。

2.如申請專利範圍第 1 項所述之資料保護方法，其中更包含將與第一輸出加密資料相同編碼規則之一第二輸入資料透過該流程控制器之轉傳來進行該解密動作，進而與該第一輸出加密資料一併還原成該第一輸出解密資料。

3.如申請專利範圍第 1 項所述之資料保護方法，其中該第一輸出加密資料中部份資料可供使用者進行檢視，但部份資料被隱藏。

4.如申請專利範圍第 1 項所述之資料保護方法，其中該第二輸出資料再透過該流程控制器之轉傳而進行另一加密動作，進而產生一第二輸出加密資料。

5.如申請專利範圍第 4 項所述之資料保護方法，其中該第二輸出加密資料中部份資料可供使用者進行檢視，但部份資料被隱藏。

6.如申請專利範圍第 4 項所述之資料保護方法，其中將該第二輸出加密資料透過該流程控制器之轉傳來進行另一解密動作，進而還原成一第二輸出解密資料，然後再將該第二輸出解密資料進行一第三處理步驟而產生一第三輸出資料。

7.如申請專利範圍第 6 項所述之資料保護方法，其中可將該第三輸出資料儲存於一記憶體裝置中。

8.如申請專利範圍第 1 項所述之資料保護方法，其中該工具程式係為一控制晶片之程式碼開發程式。

9.如申請專利範圍第 1 項所述之資料保護方法，其中使用者通過解讀或編輯該中間資料以解讀或編輯該工具程式的程式碼。

10.一種資料保護工具程式，用以處理經過加密之一輸入資料，包括：

複數處理單元，該複數處理單元分別進行對應之複數處理步驟；

其中，該輸入資料進行一解密步驟後執行任一處理步驟以產生一輸出資料；及

該輸出資料進行再次加密，而加密後之該輸出資料係為該等處理單元間之中間資料以供使用者存取，且該輸入資料進行該解密步驟後的資料不可被使用者存取。

11.如申請專利範圍第 10 項所述之資料保護工具程式，其中該輸出資料於再次加密後自與執行之該處理步驟對應之該處理單元輸出。

12.如申請專利範圍第 11 項所述之資料保護工具程式，其中該輸出資料為另一處理單元之該輸入資料。

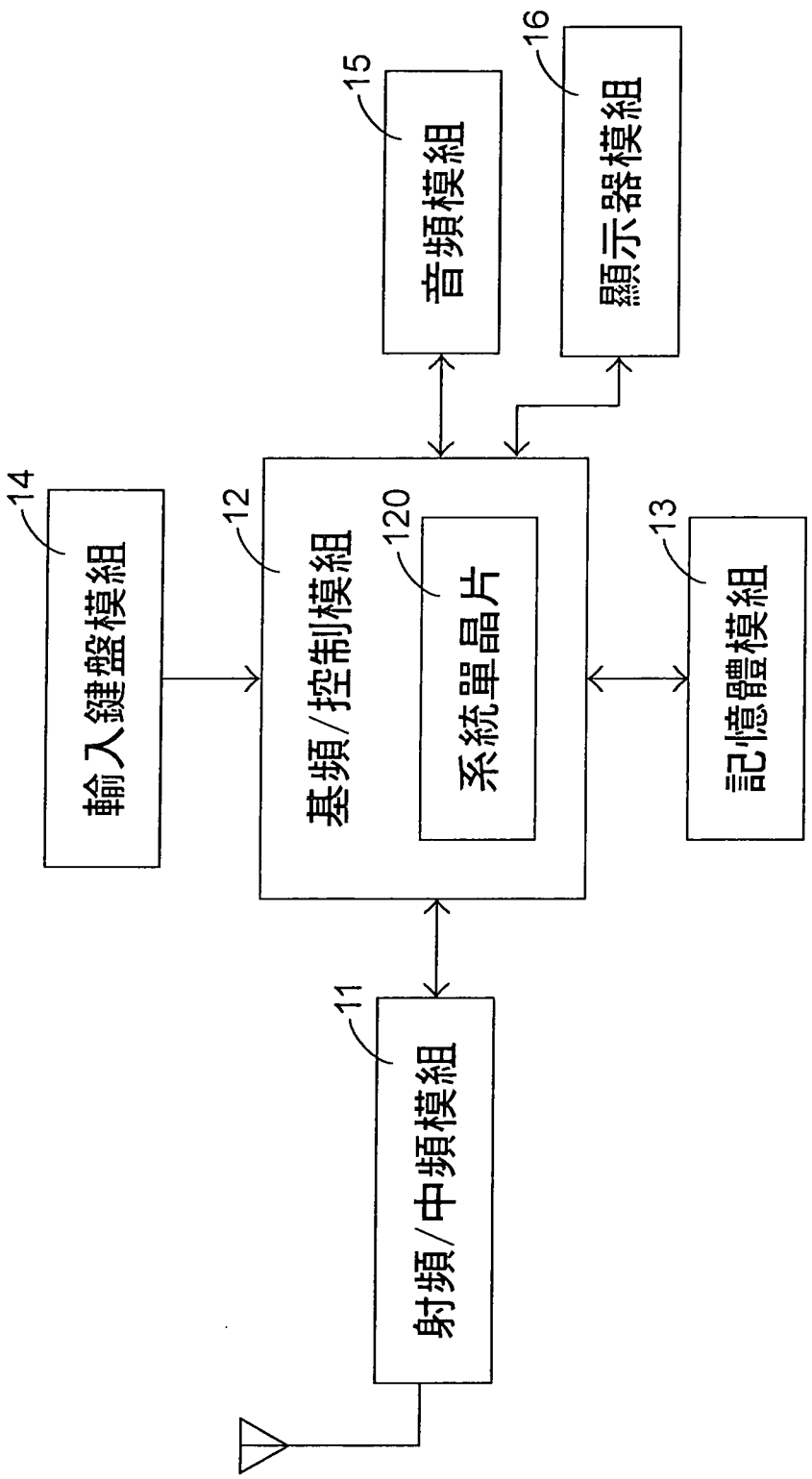
13.如申請專利範圍第 12 項所述之資料保護工具程式，其中該輸入資料進行一解密步驟後執行任一處理步驟以產生另一輸出資料；及

該輸出資料進行再次加密。

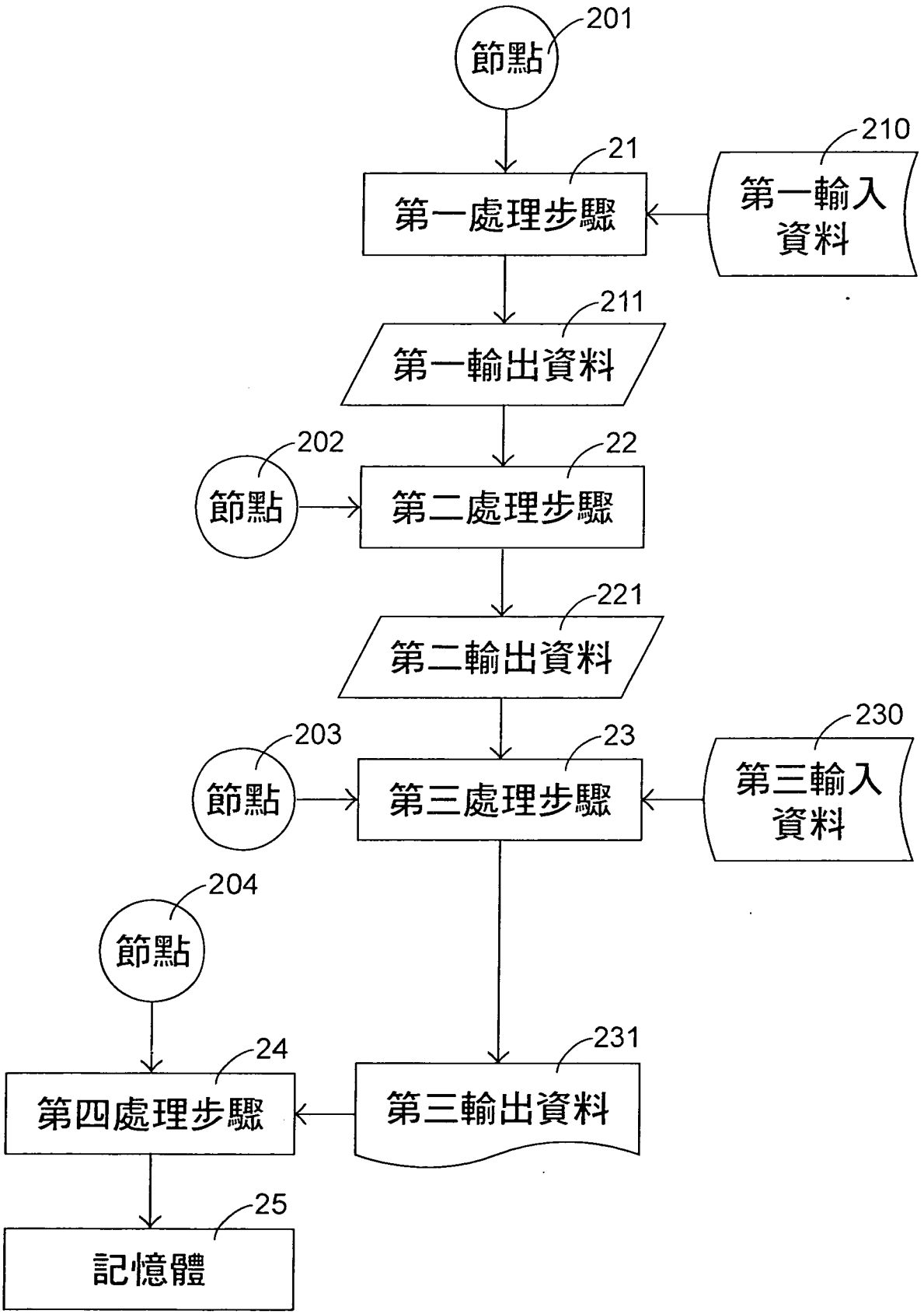
14.如申請專利範圍第 10 項所述之資料保護工具程式，其中自該資料保護工具程式輸出之該輸出資料為加密的狀態。

15.如申請專利範圍第 10 項所述之資料保護工具程式，其中使用者通過解讀或編輯該中間資料以解讀或編輯該資料保護工具程式的程式碼。

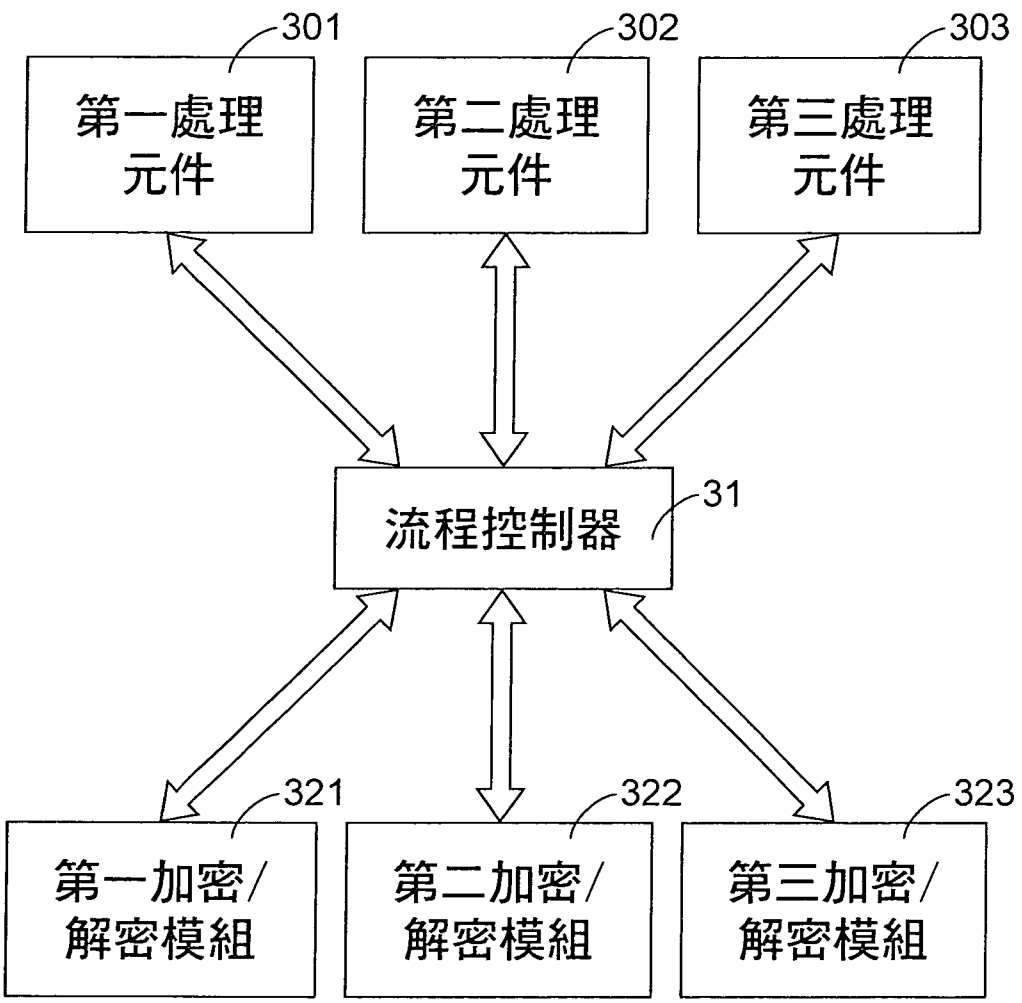
十一、圖式：


15
音頻模組
16
顯示器模組
14
輸入鍵盤模組
12
基頻/控制模組
120
系統單晶片
13
記憶體模組
11
射頻/中頻模組

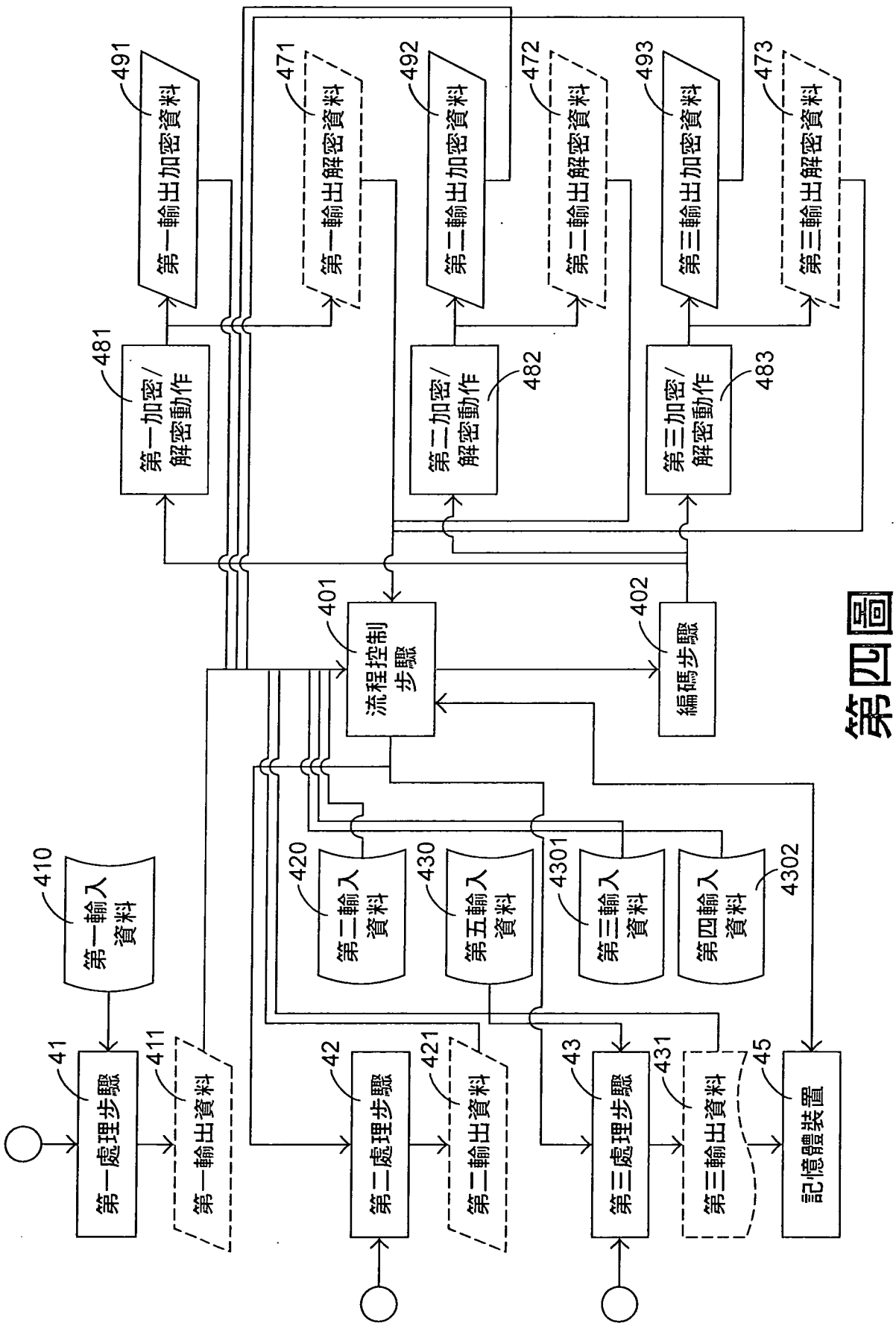
第一圖


節點
201
210
21
第一處理步驟
第一輸入資料
211
第一輸出資料
202
22
節點
第二處理步驟
221
第二輸出資料
230
203
23
節點
第三處理步驟
第三輸入資料
204
節點
24
231
第四處理步驟
第三輸出資料
25
記憶體

第二圖


301
302
303
第一處理元件
第二處理元件
第三處理元件
流程控制器
31
321
322
323
第一加密/解密模組
第二加密/解密模組
第三加密/解密模組

第三圖


第一處理步驟
第二處理步驟
第三處理步驟
第三輸出資料
記憶體裝置
第一輸入資料
第二輸入資料
第五輸入資料
第三輸入資料
第四輸入資料
第一輸出資料
第二輸出資料
流程控制步驟
編碼步驟
第一加密/解密動作
第二加密/解密動作
第三加密/解密動作
第一輸出加密資料
第一輸出解密資料
第二輸出加密資料
第二輸出解密資料
第三輸出加密資料
第三輸出解密資料
41
42
43
45
401
402
410
411
420
421
430
431
4301
4302
471
472
473
481
482
483
491
492
493

第四圖